(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 327 937 A1

(12) EUROPEAN PATENT APPLICATION

published in accordance with Art. 158(3) EPC

(43) Date of publication:
16.07.2003 Bulletin 2003/29

(21) Application number: **00961119.5**

(22) Date of filing: **20.09.2000**

(51) Int Cl.[7]: **G06F 12/14**, G06F 12/00, G06F 13/00

(86) International application number:
PCT/JP00/06420

(87) International publication number:
WO 02/027501 (04.04.2002 Gazette 2002/12)

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(71) Applicant: **Yasukura, Yutaka**
Tokyo-to 151-0072 (JP)

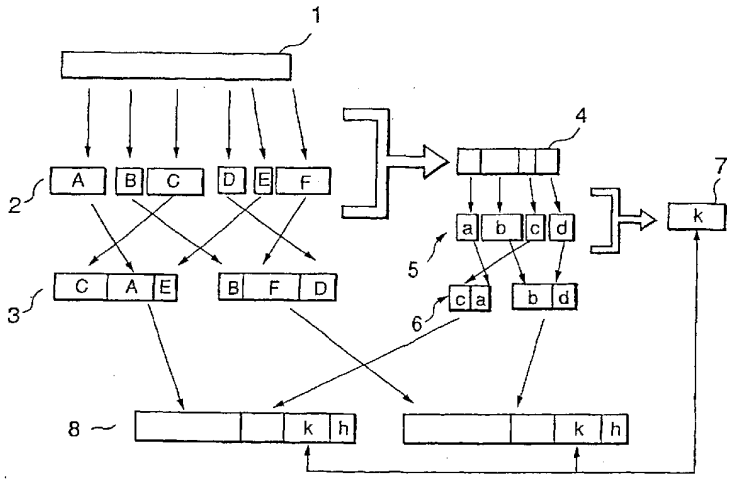
(72) Inventor: **Yasukura, Yutaka**
Tokyo-to 151-0072 (JP)

(74) Representative: **Patentanwälte**
Leinweber & Zimmermann
Rosental 7,
II Aufgang
80331 München (DE)

(54) METHOD OF EDITING/RESTORING ELECTRONIC INFORMATION

(57) An electronic information file (1) is divided into a plurality of information elements (2), which are combined in different orders to generate two or more information blocks (3) and to generate a primary distribution information file (4) holding information on the method for dividing/rearranging the information elements (2). Like the electronic information file (1), the primary distribution information file (4) is divided into key fragments (5) and rearranging to generate key blocks (6) and to generate a secondary distribution information file (7) holding information on the method for dividing/rearranging the primary distribution information file. The information blocks (3), the key blocks (6) and the secondary distribution information file (7) are combined to generate and store to transmit two or more packages (8). When the electronic information is used, the primary distribution information file (4) is restored on the basis of the secondary distribution file (7) to restore the electronic information file (1) on the basis of the primary distribution information file (4).

FIG.1



EP 1 327 937 A1

Description

Field of the Invention

[0001] The present invention concerns a security method of electronic information in storage or communication of electronic information.

Background Art

[0002] As a number of computers are connected to the communication network and composing a system, each computer has become possible to be linked with the general public through the communication channel. Therefore, it is feared that even electronic information stored in a hard disk or other computer external memory storages be accessed by unauthorized outsiders through the communication channel, then stolen or altered.

[0003] Besides, electronic information comes often to be transmitted using a communication channel, as shown in exchange of personal informations such as electronic mail, credit card number, password, distributions of application programs such as game program, business program, and of data extracted for edit from a database.

[0004] In case of using a communication environment open to the outside for such electronic information exchange, an outsider who is not the receiver may acquire and use the electronic information during communication by interception or theft act. Especially, in case of distributing charged information or transmitting information involving the privacy, it is necessary to prevent electronic information during communication from being stolen easily.

[0005] Methods for securing the confidentiality of electronic information by the encryption are executed, because it is enough that the unrelated outside cannot use the electronic information even if it is acquired during communication or storage. The encryption technology developed for such effect exists variously for the encryption methods using symmetric keys, and for the encryption methods using asymmetric keys.

[0006] However, even when these encryption technologies are used, any person who would have acquired a decryption method by deciphering the encryption or by any means can restore easily and obtain useful information, as long as the whole information is contained in the stored electronic information or the transmitted electronic information. Moreover, the information may be altered or falsified, so we should always worry if the electronic information retrieved or received maintains the genuine information or not. Especially, the conventional method is uncertain, in case of storing or transmitting an electronic information requiring a high level of concealment, high level personal secret information or company secret information and so on.

[0007] There, the inventor of the invention has already disclosed by PCT/JP99/01350 a method for dividing an electronic information file into a number of information elements, combining them in different orders to generate several information blocks and sending them individually or storing them in external memory storages individually. During the generation of information blocks, division/extraction data is created which holds information concerning the size of respective information elements, the order of combination of information elements and so on, the information blocks and the divisionlextraction data are sent individually or stored in external memory storages individually. When the electronic information file is restored, information elements in the information blocks are cut out, rearranged and bonded in the correct order.

[0008] According to this method, information held by an individual information block is nothing but a part of the whole electronic information, and but a gathering of divided fragments, whose information value is diminished even if the information block is stolen.

[0009] Nevertheless, in case where the division/extraction data was stolen together with some information blocks and the information etements in the information block could be rearranged correctly, at least a part of information would be known correctly by the interceptor.

[0010] On the other hand, the division/extraction data describes the position of each information element in the original electronic information file. Consequently, in case where the division/extraction data and any information blocks were stolen, the interceptor could know correctly which the position is in the original electronic information file that corresponds to the information element in the stolen information blocks, therefore, the interceptor can acquire a fragment of the useful information or a clue to infer the whole picture of the original electronic information.

Disclosure of the Invention

[0011] The method of editing/restoring electronic information divides an electronic information file into a number of information elements, selects an arbitrary information element from divided information elements, and combines them in a different order to generate two or more information blocks. These information blocks are composed to include all information elements, if all information blocks are integrated. On the other hand, a primary distribution information file is created which records the method for dividing into information elements and the method for forming information blocks. Furthermore, the primary distribution information file is divided similarly into a number of key fragments and redistributed to create key blocks, and a secondary distribution information file is created which records the method for dividing into key fragments and the method for forming the key block.

[0012] The key block and the secondary distribution

information file are optionally attached to the information blocks to form two or more packages, to be sent individually to the receiver or stored in external memory storages. It should be appreciated that, when the package is created, it is so composed that all information blocks and key blocks will be contained if all packages are integrated. Besides, the secondary distribution information file may be divided in a style capable of restoring easily, and then contained in a part or all packages.

[0013] When the electronic information is used, the secondary distribution information file is cut out from the packages, the key blocks contained in the packages are re-divided into key fragments based on the secondary distribution information file, and rearranged and bonded in the correct order to restore the primary distribution information file. Further, the information elements are re-divided and bonded similarly from the information blocks in the packages based on the primary distribution information file.

[0014] According to the method of editing/restoring electronic information of the present invention, the information elements would not be cut out from the information blocks and the information would not be restored correctly, even when some of packages and the secondary distribution information file were stolen, because the primary distribution information file can not be restored, as far as all packages are not stolen. In addition, the thief can not restore even a part of the information from the stolen packages nor infer the whole picture of the electronic information, because they cannot know the corresponding position of the stolen information in the whole electronic information as far as the primary distribution information file is not restored.

[0015] Consequently, as the primary distribution information file is divided, it is extremely difficult to restore or infer the information even if some of packages are stolen, and the possibility of plagiarism of the information is extremely low; therefore, the information security can be secured certainly, by using the method of editing/restoring electronic information of the present invention.

[0016] It should be noted that, it is unnecessary to take care strictly the secondary distribution information file, and any special problem will not occur without division, encrypting or other processing of the secondary distribution information file, because the information block could not be restored correctly so long as the primary distribution information file be not restored, even if the secondary distribution information file was stolen.

[0017] When the method of editing/restoring electronic information of the present invention is used for on-line sale of application programs or data base, even if a person other than the rightful purchaser steals electronic information during the communication, he can not restore the data; therefore, he can not execute the program, or acquire an useful information. Consequently, as there is no motive for stealing electronic information during the communication, the benefit of a vendor would not be damaged by the theft.

[0018] Also, when it is applied to an extremely secure information exchange can be realized, because even a part of the date could not be restore even if the electronic information is stolen.

Brief Description of Drawings

[0019]

Fig. 1 is a bock diagram illustrating procedures for the transmission end in a method of editing/restoring electronic information of the present invention;
Fig. 2 is a flow diagram showing procedures for the transmission end in a method of security confirmation of the present invention;
Fig. 3 is a bock diagram illustrating procedures for the receiving end in a method of editing/restoring electronic information of the present invention; and
Fig. 4 is a flow diagram showing procedures for the receiving end in a method of security confirmation of the present invention.

Best Mode for Carrying out the Invention

[0020] The method of editing/restoring electronic information of the present invention is a method for securing the security of electronic information in storage or communication of electronic information. The method of the present invention is capable of diminishing the value that the information has and prevents the damage of theft by making difficult to restore or infer the information that can be acquired by plagiarism, even if someone steals an electronic information in the course of storage or communication.

[0021] Now, the invention shall be described in detail referring to drawings.

[0022] Fig. 1 is a bock diagram illustrating a method for editing electronic information in a method of editing/restoring electronic information of the present invention. Besides, Fig. 2 is a flow diagram showing procedures for editing electronic information of the present invention. For the convenience of description, a case is illustrated where an electronic information file is divided into six information elements and allotted to two information blocks.

[0023] In the method for editing electronic information of the present invention, an object electronic information file 1 is taken in (s1) and divided into an appropriate number of information elements 2 (s2). Here, for simplicity, it is divided into six information elements A, B, C, D, E, and F. The information elements 2 are not necessary to be divided at such positions so as to have meaning information, but those obtained simply by dividing physically the electronic information file 1 are preferable, in order to reduce the danger in the case where they are plagiarized.

[0024] The order of arrangement of divided informa-

tion elements A, B, C, D, E and F is changed to form an appropriate number, two in this case, of information blocks 3 by grouping conveniently (s3).

[0025] In the illustrated example, information elements A, D, E are distributed to the first information block 3 and information elements B, C, F are distributed to the second information block 3. The number of information elements in the information block 3 and the order of arrangement thereof also can be selected arbitrarily.

[0026] At the same time as the formation of the information block 3, is created which records the length information of respective information elements 2, the order of integration into the information block 3 and so on (s4).

[0027] The 5 by an operation similar to the electronic information file 1 (s5), and distributed to key blocks 6 (s6). In this example, it is divided into four key fragments, and distributed to two key blocks (c, a), (b, d). However, the number of division of key fragment or the order of distribution to key blocks also can be selected arbitrarily. It is preferred to form the same number of key blocks as information blocks 3.

[0028] Further, is created which records the length information of key fragments 5, the order of integration into the key blocks 6 and so on (s7). The secondary distribution information file 7 is indicated by a symbol k in the drawing.

[0029] Thus created information blocks 3, key blocks 6 and secondary distribution information file 7 are combined arbitrarily to form two or more packages 8 (s8) and sent individually to the receiver or store in external memory storages (s9). For the security, it is preferable to send each package via different communication channel, or to store in another storage device.

[0030] For instance, one of packages 8 holds the information elements C, A, E, the key fragments b, d and the secondary distribution information file k, the other of packages 8 holds the information elements B, F, D, the key fragments c, a and the secondary distribution information file k. Also, each package 8 is accompanied by a header h identifying the structure of contained information.

[0031] For the packages 8 having such composition, for example in case of the second package, the information held by the respective information elements B, F, D are nothing but a tiny part of the original electronic information file 1 and, moreover, even when a part of the primary distribution information file 4 is restored using the key fragments c, a based on the secondary distribution information file k, it is impossible to infer the dividing positions of the information elements B, F, D in the information block 3, the. relation between respective one of information elements B, F, D, the positions in the electronic information file 1 which located by the information held in the individual information elements and so on.

[0032] Information that can be obtained from a single package 8 becomes extremely small because the restoration of the original electronic information is made almost impossible; by dividing and extracting not only the original electronic information, but also the distribution information of electronic information in this way.

[0033] In general, information is stolen often during transmission or storage; however, in the method of editing electronic information of the present invention, the electronic information is transmitted or stored in a state of package 8; consequently, the value of information is diminished considerably even if it is stolen by an outsider, weakening the motive for plagiarizing information and lowering the danger of plagiarism

[0034] Fig. 3 is a bock diagram illustrating a method of restoring electronic information of the present invention. And, Fig. 4 is a flow diagram showing procedures for restoring electronic information of the present invention.

[0035] The user of electronic information acquires each packages 8 from the storage destination or receives them from the sender (s10), gathers all of packages 8 (s11), and cuts out first the secondary distribution information file 7 referring to the header of the packages 8 (s12). The secondary distribution information file 7 stores information concerning the order of integration of key fragments 5 into the key blocks 6, the length information and so on, therefore, the key fragments 5 are cut out from the key block 6 portion of the package 8 (s13), and rearranged to restore the primary distribution information file 4 (s14).

[0036] As the primary distribution information file 4 stores information such as the order of integration of information elements 2 into the information block 3, length of respective information elements 2 and so on, the information elements 2 are cut out based thereon (s15), rearranged to restore the original electronic information file 1, and then the original electronic information is restored (s16).

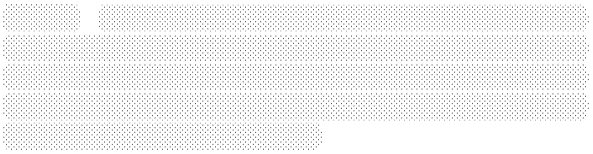
[0037] As mentioned hereinabove, in the method of editing/restoring electronic information of the present invention, the information can be sent and stored securely, because the information that can be obtained from the package is extremely small, even when the package 8 is stolen during communications or storage.

[0038] It goes without saying that the secondary distribution information file k may be contained in any of packages. Also, the secondary distribution information file k may be stored or sent separately from the packages 8.

[0039] In the method of editing/restoring electronic information of the present invention, the number of information blocks 3 corresponding to a single electronic information file 1 is not limited to two, but it may be three or more. Similarly, the number of key blocks 6 or packages 8 is not limited to two. Also, it is unnecessary that all packages 8 contain both information blocks 3 and key blocks 6. However, from the viewpoint of security, it is preferable that all packages 8 contain a key block 6. Fur-

thermore, the secondary distribution information file 7 may be divided by a style capable of restoring easily, then distributed and attached to a number of packages 8.

CPU is inherent



[0041] As mentioned in detail hereinabove, as the method of editing/restoring electronic information of the present invention, divides an electronic information file into information elements, rearranges and store separately in information blocks, creates a primary distribution information file holding information about this method of division and rearrangement, divides the primary distribution information file into key fragments, creates a secondary distribution information file holding information about the method of division and rearrangement of the primary distribution information file, generates two or more packages by containing conveniently information blocks together with key blocks and the secondary distribution information file, and puts in a communication channel or stores in a storage device, even when an outsider steals information blocks in the course of communication or storage, they can not decipher the contents of the electronic information, because small information elements are stored in pieces, allowing to prevent the secret from leaking.

Claims

1. A method of editing electronic information; comprising steps of, dividing an electronic information file into a number of information elements, generating two or more information blocks that would contain all information elements if all information blocks are integrated by selecting divided information elements and combining in different order, and also, generating a primary distribution information file recording said method of division into said information elements and formation information of information blocks, dividing the primary distribution information file into a number of key fragments, generating two of more key blocks that would contain all key fragments if all key blocks are integrated by selecting the divided key fragments and combining in different order, generating a secondary distribution information file recording information of said key fragments and forming information of said key blocks, creating a number of packages by packaging together with said information blocks and key blocks, or together with said information blocks, the key blocks and the secondary distribution information file, and storing or transmitting the packages individually.

2. A method of restoring electronic information; comprising steps of, assembling the packages edited by the method of editing electronic information of claim 1 by receiving or reading out them all, cutting out the secondary distribution information file from the packages, restoring the primary distribution information file by re-dividing the key fragments contained in the key blocks based on the secondary distribution information file to rearrange and integrate in a correct order, and at the same time, restoring the electronic information file by re-dividing information elements contained in the information blocks based on the primary distribution information file to rearrange and integrate in the correct order.

3. A computer readable recording medium for recording a program for executing, by a computer, of procedures of, dividing an electronic information file into a number of information elements, generating two or more information blocks that would. contain all information elements if all information blocks are integrated by selecting the divided information elements and combining in different order, generating a primary distribution information file recording formation information of the information elements and the information blocks, dividing the primary distribution information file into a number of key fragments, generating two of more key blocks that would contain all key fragments if all key blocks are integrated by selecting divided the key fragments and combining in different order, generating a secondary distribution information file recording said forming information of key fragments and key blocks, creating a number of packages by packaging together with said information blocks and key blocks, or said information block, key blocks and the secondary distribution information file, and storing or transmitting the packages individually.

4. A computer readable recording medium for recording a program for executing, by a computer, of procedures of, assembling the packages edited based on the program of claim 3 by receiving or reading out them all, cutting out the secondary distribution information file from the package, restoring the primary distribution information file by re-dividing the key fragments contained in the key block based on the secondary distribution information file to rearrange and integrate in a correct order, and at the same time, restoring the electronic information file by re-dividing information elements contained in the information block based on the primary distribution information file to rearrange and integrate in a correct order.

FIG.1

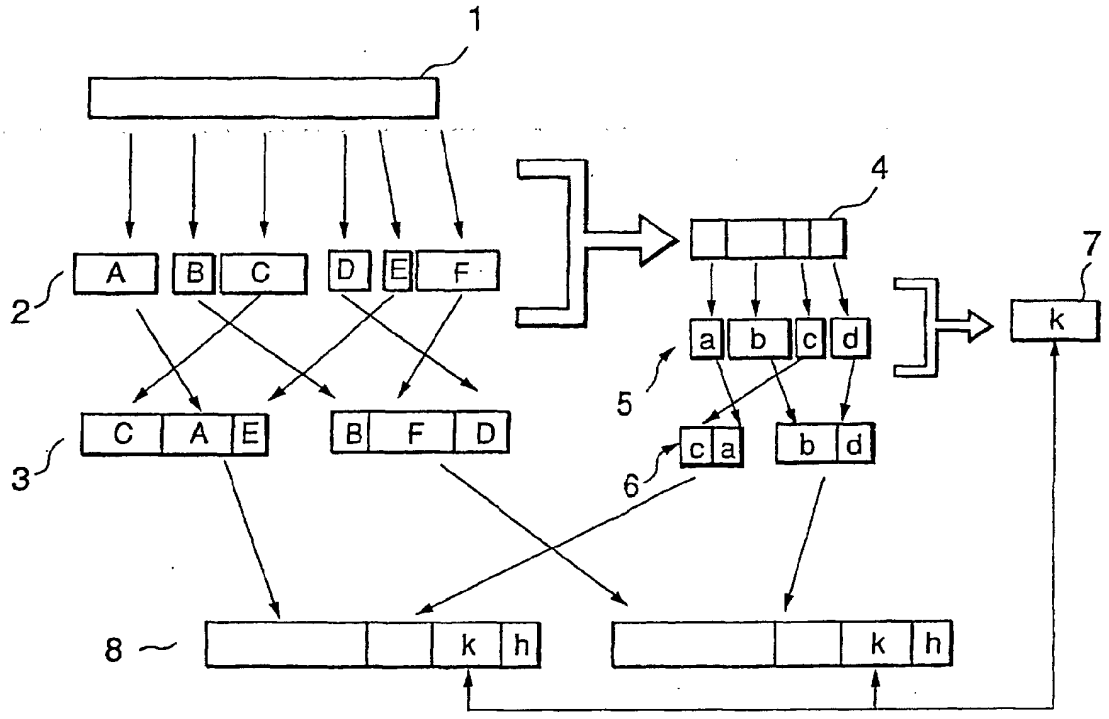


FIG. 2

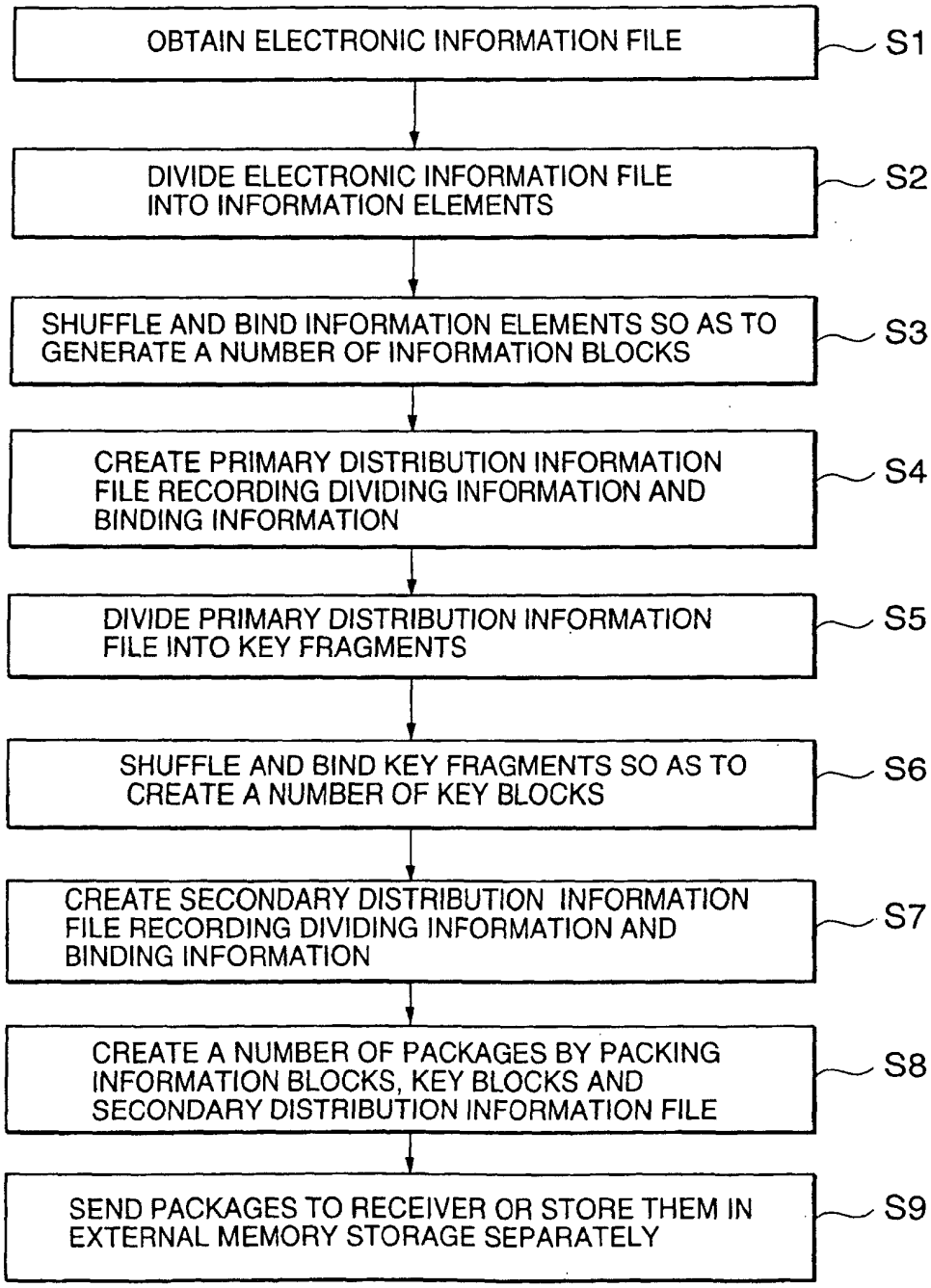

OBTAIN ELECTRONIC INFORMATION FILE
S1
DIVIDE ELECTRONIC INFORMATION FILE INTO INFORMATION ELEMENTS
S2
SHUFFLE AND BIND INFORMATION ELEMENTS SO AS TO GENERATE A NUMBER OF INFORMATION BLOCKS
S3
CREATE PRIMARY DISTRIBUTION INFORMATION FILE RECORDING DIVIDING INFORMATION AND BINDING INFORMATION
S4
DIVIDE PRIMARY DISTRIBUTION INFORMATION FILE INTO KEY FRAGMENTS
S5
SHUFFLE AND BIND KEY FRAGMENTS SO AS TO CREATE A NUMBER OF KEY BLOCKS
S6
CREATE SECONDARY DISTRIBUTION INFORMATION FILE RECORDING DIVIDING INFORMATION AND BINDING INFORMATION
S7
CREATE A NUMBER OF PACKAGES BY PACKING INFORMATION BLOCKS, KEY BLOCKS AND SECONDARY DISTRIBUTION INFORMATION FILE
S8
SEND PACKAGES TO RECEIVER OR STORE THEM IN EXTERNAL MEMORY STORAGE SEPARATELY
S9

FIG.3

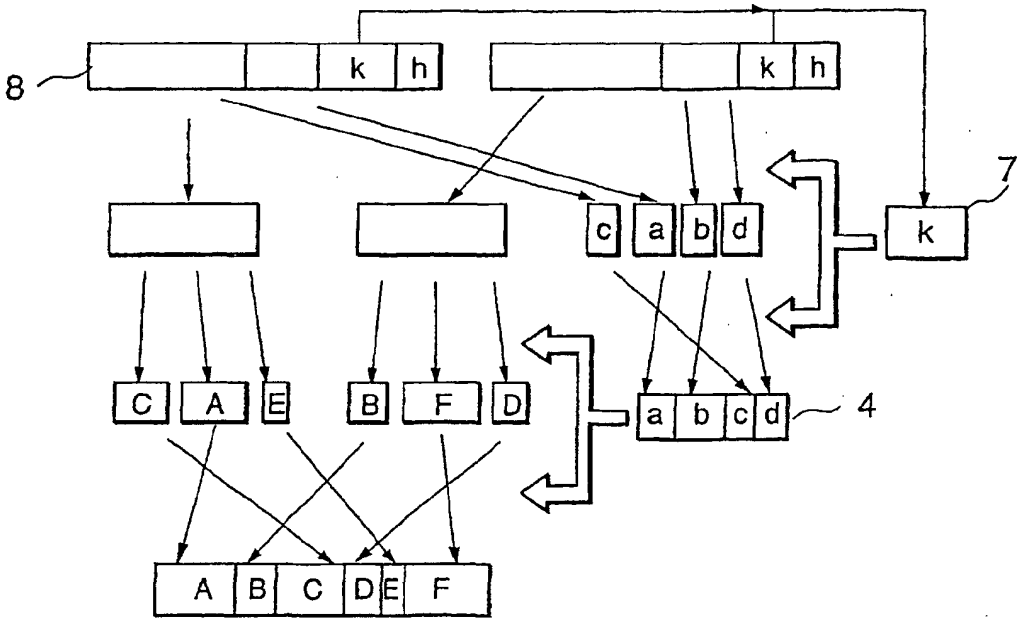
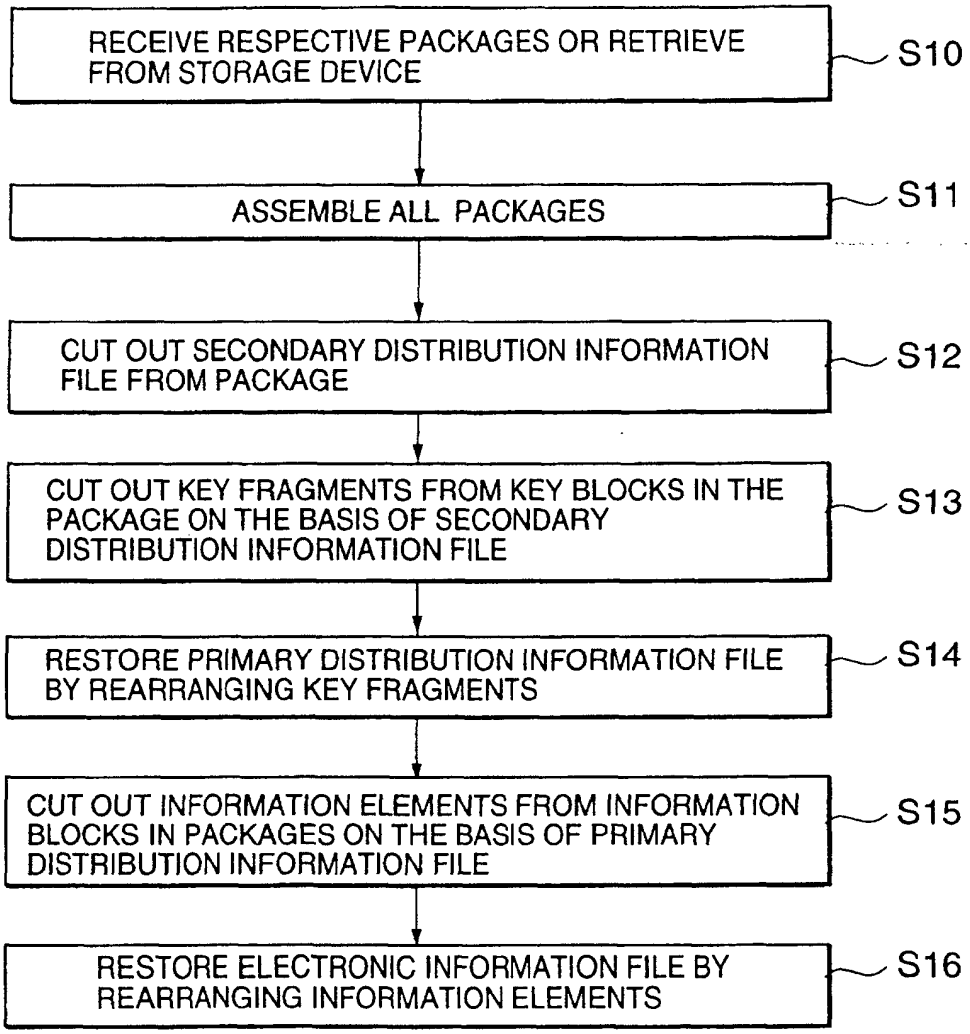


FIG. 4


RECEIVE RESPECTIVE PACKAGES OR RETRIEVE FROM STORAGE DEVICE
S10
ASSEMBLE ALL PACKAGES
S11
CUT OUT SECONDARY DISTRIBUTION INFORMATION FILE FROM PACKAGE
S12
CUT OUT KEY FRAGMENTS FROM KEY BLOCKS IN THE PACKAGE ON THE BASIS OF SECONDARY DISTRIBUTION INFORMATION FILE
S13
RESTORE PRIMARY DISTRIBUTION INFORMATION FILE BY REARRANGING KEY FRAGMENTS
S14
CUT OUT INFORMATION ELEMENTS FROM INFORMATION BLOCKS IN PACKAGES ON THE BASIS OF PRIMARY DISTRIBUTION INFORMATION FILE
S15
RESTORE ELECTRONIC INFORMATION FILE BY REARRANGING INFORMATION ELEMENTS
S16

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP00/06420

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] G06F12/14, G06F12/00, G06F13/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] G06F12/14, G06F12/00, G06F13/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2000
Kokai Jitsuyo Shinan Koho 1971-2000 Jitsuyo Shinan Toroku Koho 1996-2000

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JP 9-293021 A (International Business Machines Corporation), 11 November, 1997 (11.11.97), & KR 97066880 A & US 5870468 A	1-4
A	JP 4-184476 A (Hitachi, Ltd.), 01 July, 1992 (01.07.92), (Family: none)	1-4

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
18 December, 2000 (18.12.00)	26 December, 2000 (26.12.00)
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

Form PCT/ISA/210 (second sheet) (July 1992)